Survey on Cloud Computing Security Issues

Amanpreet Kaur Sara*

Abstract

In today's reality the most recent pattern in IT is cloud computing. Cloud computing is not another thought but rather has some new features, for example, low expenditure, quick arrangement and trustworthy services. It is a developing innovation in light of grid computing, parallel computing, distributing computing and virtualization. The cloud computing give a chance to IT sector part by opening up another boulevard of giving cloud based services to worldwide associations running from SaaS based application services and remote application facilitating services. The most essential consideration toward any business association is security. Security is exceptionally troublesome assignment to execute at each level in cloud design framework. Hazard distinguishing proof and investigation is vital to organize the usage (degree and time allotment) of governance and controls, and to build up extension for looking into or reviewing cloud computing situations. In view of the noticeable proof and analysis of risk, controls ought to be outlined and executed to guarantee that vital moves are made to control risks and to accomplish business and IT goals. The main objective of this survey paper is on mitigations for cloud computing security challenges as a principal step towards assuring secure cloud computing environment.

Keywords: security challenges; cloud computing; Risks; mitigation.

I. Introduction

The IT world develops from mainframes computers to client servers, the Internet, virtualization and cloud computing. The Cloud Computing is most rising IT business innovation. By "Cloud computing gives a mutual pool of configurable IT services. According to NIST "Cloud computing provides a shared pool of configurable IT resources (e.g. processing, network, software, information and storage) on demand, as a scalable and elastic service, through a networked infrastructure, based upon (pay-per-use or subscription), which require minimal management effort, is mainly based upon service level agreements between the cloud service provider and users, and frequently utilizes virtualization resources". [1]With the change in time as the IT industry achieve its heights it also captured by many risks these risk acts as main obstacle to a organization to transfer its data/ information to cloud . We will discuss these risks and challenges in the coming section.

II. Literature Survey

A. Cloud Computing:

The NIST Definition of Cloud Computing Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]Cloud computing, also known as a pool of resources, where we can use resources as on demand with the use of internet through some tools without contacting to the server.[2]

B. Essential characteristics of Cloud Computing:

Five important characteristics of Cloud Computing are explained as under:

- On-demand-self-service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

On-demand-self-service:
Client can profit or leave the services as he or she want whenever on the premise of their requests without dealing the service provider.

Broad Network Access:
It has capacity over the n/w and got to through standard mechanism that promote use via heterogeneous slim or thick customer platforms, for example, cellular telephones, tablets and PDAs.

Amanpreet Kaur Sara*
Department of IT
Institute of Information Technology and
Management, GGSIPU, Delhi, India

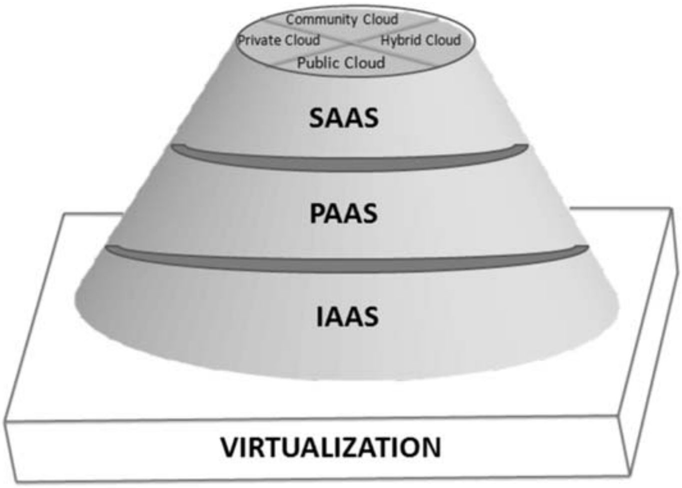

Fig. 1: Cloud Computing Model

Resource Pooling:

It's a pool of services of computing resources so that multiple customer can use it with lowest cost or we can say that we it reduces the infrastructure cost.

Rapid Elasticity:

Capabilities can be flexibly avail and discharged, now and again naturally, proportional quickly outward and internal similar with interest. To the buyer, the capacities accessible for provisioning regularly have all the earmarks of being boundless and can be appropriated in any amount whenever.[1]

Measured Service:

Cloud computing frameworks consequently control and streamline resource utilization by giving a metering ability to the kind of services (e.g. storage, processing, bandwidth, or active user accounts) (Cloud Security Alliance, 2009, p15).

C. Cloud Computing Services Model :

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)

SaaS (Software as a Service):

Model is referred as on-demand software service. You don't need to stress over the establishment, setup and execution of the application. Cloud provider will do that for you. You simply need to pay and utilize it through some customer. e.g.: Google Apps, Microsoft Office 365.[2]

PaaS (Platform as a Service):

As the name recommends, gives you platform for computing which ordinarily incorporates operating

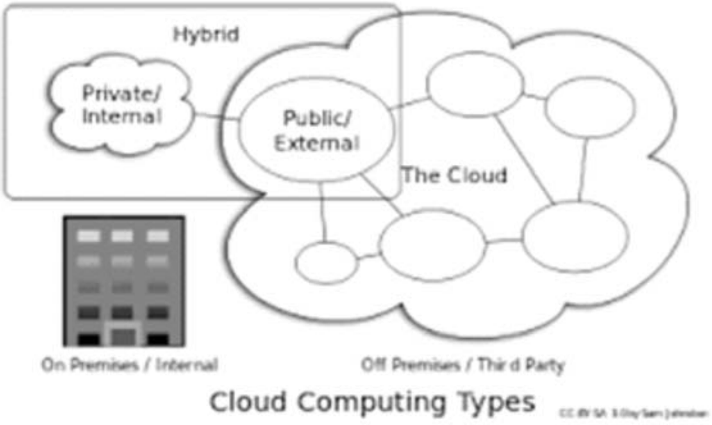

Fig. 2: Deployment models [15]

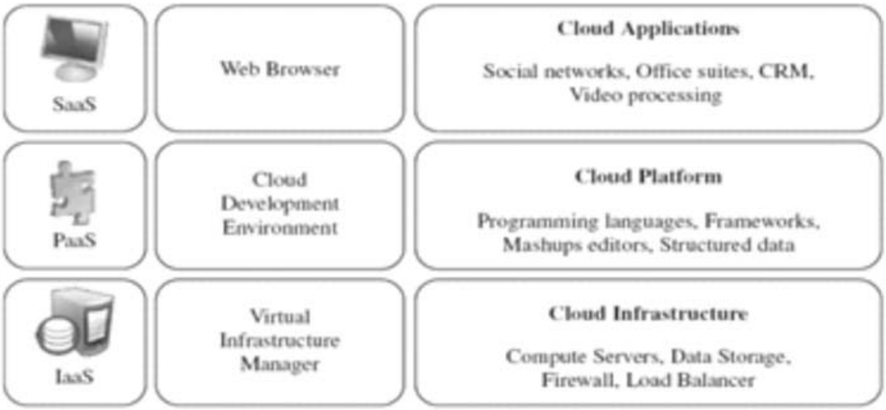
SaaS
Web Browser
Cloud Applications
Social networks, Office suites, CRM, Video processing
PaaS
Cloud Development Environment
Cloud Platform
Programming languages, Frameworks, Mashups editors, Structured data
IaaS
Virtual Infrastructure Manager
Cloud Infrastructure
Compute Servers, Data Storage, Firewall, Load Balancer

Fig. 3: Services Models [3]

systems, execution of various programming applications, databases and many more e.g.: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.

IaaS (Infrastructure as a Service):
As the name recommends, gives you the infrastructure, physical or virtual machines (VMS) and many other resources e.g.: Amazon EC2, Windows Azure, Rackspace, and Google Compute Engine.

D. Cloud Computing Deployment Model:

With reference to NSIT the cloud services can be deployed with help of various models which are explained as under:

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

The definitions of the deployment models listed next are taken as it is from the NIST definition, although other researches mention this deployment models with similar definitions.[6]

Private Cloud:
The cloud infrastructure is worked exclusively for an association. It might be overseen by the association or an outsider.

Public Cloud:
The cloud infrastructure is made accessible to the common public or a large industry group and is owned by an organization selling cloud services.

Hybrid Cloud:
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Community Cloud:
The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party.

E. Cloud computing Risks:

Despite the fact that there are numerous drivers for moving to a cloud based arrangement, cloud computing is not without risk or totally secure. The cloud threats connected with every cloud conveyance model change and are reliant on an extensive variety of factors including the sensitivity of resources of information, cloud architectures and security controls included in a specific cloud environment. An intensive comprehension and the change of security risk speak to essential steps towards securing cloud environment and binding the advantages of cloud computing [5]. Taking after is cloud computing recognized security risks:

- Data security risks
- Administration and control security risks
- Logical access security risks

- Network security risks
- Physical access security risks
- Compliance security risks
- Virtualization security risks.

Data security, Administration and control:

Information security risk establish the greatest obstacle for cloud computing. Data/information security is a vital viewpoint while information/data in travel/ transit, processed and stored. A few organizations are still hesitant to move information/data and applications to the cloud, particularly if basic to the business, because of the danger of information/data spillage prompting privately and security risks , the absence of control over facilitated information/data and applications, accessibility worries of cloud administrations and information, the risk of information/data uprightness hindrance, and ineffectual assurance of information in travel/transit , in rest or in backup because of insufficient encryption.

Data Privacy:

Challenge: The sharing of cloud structure can prompt information/data security and classification issues [5].

Solution: Information that is permitted in the cloud ought to be distinguished and arranged as needs be [5].

Data control:

Challenge:

As the organization does not have any straight control over data being hosted by a cloud service provider so it not easy to protect data and to enforce privacy-identity and cyber-crime security.

Solution:

External audits should be performed on a regular basis to monitor the cloud service provider's compliance to contracted terms and the effective execution of security policies, procedures and Standards.

Availability of data and services:

Challenge: Failure of recovery processes and tested plans are critical in the event of a failure to ensure availability of services and data.

Solution: Data must be available and data back-up and recovery schemes for the cloud must be in place and effective to prevent data loss, inadequate data overwrite or destruction.

Data Integrity:

Challenge: The reliability of networks, applications, databases and system software in a shared, globally accessed cloud environment is threatened by much vulnerability when not adequately and timely patched.

Solution: Tasks for efficient patch management should be clearly defined and implemented.

Data Encryption:

Challenge: A major risk in cloud computing environments is insufficient encryption and key managing of data.

Solution: Encryption and key management should be based on industry and government Standards.

Logical access: The risks of un approved access to information/data and applications in the cloud. Access by means of an open system and facilitated administrations implies expanded disclosure and thusly more risk. Privileged access rights ought to be allocated suspiciously to approved persons just, and assessment for sufficiency all the time [5]. The execution of security devices and strategies are required to guarantee approved client access to information and applications.

Network Security:

Hacking and obstruction risk incorporate attackers accessing information/data and applications through some sort of remote access framework and web application. Assaults like to embed resentful code into standard SQL code with the goal that hackers can increase unapproved access to database or critical information /data [12]. Security risks, for example, man-in-the-center assaults, authentication. [5,12,13] Methods like sifting and proxy based servers which energetically recognize and separate clients for suspected information/data [12].

Physical Security:

The cloud administrations brought on by physical access are diverse between tremendous cloud administration suppliers and their clients. These providers ought to be knowledgeable about securing vast server farm offices and have considered flexibility among other accessibility methodologies. There is a risk that cloud client framework can be physically upset all the more effortlessly whether by insiders or remotely where less secure office situations or remote working is standard practice. [5]

Compliance:

Organizations are at last in charge of guaranteeing the security and integrity of their information, anyhow when it is held by service providers in the cloud. Association further need to demonstrate consistence with security benchmarks separated from the areas of their information/data and applications.

Virtualization:

Security risks are normal risk proficient in virtual situations. Full Virtualization and Para Virtualization are two sorts of virtualization in a cloud computing model. In full virtualization, whole hardware architecture is replicated virtually. However, in para virtualization, an operating system is modified so that it can be run concurrently with other operating systems.

Elements affecting security risks incorporate variable workloads, dynamic movement and changes, manager aptitudes, learning and preparing, access controls, antagonistic visitors, the vanishing of "edge security", multiplication of VMs, setup settings, hypervisor and VM screen layer vulnerabilities, absence of deceivability, absence of procedure administration, and VM server sprawl.

III. Conclusion

Concept of Cloud Computing brings many uncertainties to compliance with privacy regulations. So, current privacy regulations are not enough to resolve all privacy concerns related to Cloud computing. Here I gave an overview of risks to security of cloud computing. We also discussed effective mitigations, and introducing elements of security in cloud computing. Security could be one major issue in the adaptation of Cloud computing. Not many organizations are aware of privacy issues in Cloud Computing. Security issues are an active domain of research and experiment at this point in time. Research is on to address concerns related to network security, data protection, segregation of resources and virtualization.

References

1. NSIT (The NIST Definition of Cloud Computing, SP800-145.pdf)
2. http://www.investopedia.com/terms/c/cloud-computing.asp
3. W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to cloud computing," Cloud Computing, pp. 1-41, 2011
4. Security Guidance for Critical Areas of Focus in Cloud Computing, www.cloudsecurityalliance.org (last access on Dec. 2010).
5. M.Carrol,van der Merwe and P.Kotze 'Secure Cloud Computing Benefits, Risks and Controls', Information Security in South Africa (ISSA)2011, 978-1-4577-1481-8
6. C. Cachin, I. Keidar and A. Shraer, "Trusting the Cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
7. Sun, http://blogs.sun.com /gbrunett/entry/ amazon_s3_silent_data_corruption.
8. RedHat, https://rhn.redhat.com/errata/RHSA-2008-0855.html.
9. OpenID Foundation, http://openid.net/get-an-openid/individuals/, last accessed September 13 2012, 56
10. Philpott, R., Maler, E., Ragouzis, N., Hughes, J., Madsen, P., and Scavo, T.OASIS Open 2008, Security Assertion, Markup Language (SAML) V2.0 Technical Overview, Committee, Draft 02, http://docs.oasis-open.org/security/saml/post2.0/sstc-saml-tech-overview-2.0.html
11. Erdos, M., and Cantor, S. Shibboleth Architecture Protocols and Profiles, http://shibboleth.internet2.edu/shibboleth-documents.html.
12. Vahid Ashktorab2, Seyed Reza Taghizadeh1 'Security Threats and Countermeasuresin Cloud Computing', International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 1, Issue 2, October 2012 ISSN 2319 – 4847
13. "Sara Qaisar", 'Cloud computing: Network/Security threats and countermeasures' interdisciplinary journal of on temporary research in business January 2012 vol 3, no 9.
14. https://en.wikipedia.org/wiki/Cloud_computing